RESPONSE

SCREEN SCRAPING – POLICY AND REGULATORY IMPLICATIONS

23 October 2023

EXECUTIVE SUMMARY

CashDeck is one of the largest providers of bank data to finance brokers in Australia. Our service is used in an estimated 15-25% of all broker-originated mortgages to help these brokers meet their obligations under the National Consumer Credit Protection Act 2009 and RG 273 (Mortgage Brokers: Best Interest Duty) whilst also providing them documentation required by lenders as part of loan applications. To provide this service, we rely heavily on data only available via screen scraping.

CashDeck supports the eventual move away from screen scraping to CDR-derived data. Unfortunately, CDR is still not suitable for use by our primary clients, mortgage brokers, for three major reasons (for more detail, see the answers to specific questions raised in the consultation paper later in this document):

1. Data is missing from CDR including official statement PDFs (that are often required as part of the loan application process), certain data holders (buy now pay later, small/medium account credit contract providers & certain charge card products like American Express) and certain business account types.

2. Significantly increased friction from clients, especially around the consent of joint and business accounts. A very common inclusion in mortgage broker-originated loans as there are over 2.5 million Australian businesses, all which have more complicated financial situations where mortgage brokers can provide significant value.

   CashDeck understands this is a known issue by ACCC, but there's still uncertainty as to what needs to be done to correct this moving forward and all current proposals will require significant re-engineering of consent flows by all CDR participants once this is decided.

3. Incompatibility of consent timeframes allowed in CDR for Trusted Advisers and those required as part of a broker's Australian Credit License (ACL), which is at least 7 years after the relationship has ceased.

CashDeck treats consumer data with the reverence it deserves. We encrypt all data in transit and at rest, we keep credentials separate from the rest of the consumer's data and only have access to them

for the time required to complete a retrieval, securely deleting them after. We do not have long-term access to consumer accounts.

Purchasing a property and the associated mortgage application process is among one of the most stressful times of many people's financial journey. CashDeck not only enables mortgage brokers to meet their compliance obligations, but we significantly reduce the amount of unfamiliar document collection and analysis that would otherwise be required directly by the consumer, potentially adding both days to the approval process and significant stress during an already fraught time.

Without screen scraping, mortgage brokers need to collect this data directly from clients, often receiving inaccurate, inconsistent, and heavily delayed data. Many applications require more than 50 documents to be collected from a consumer's banking portal to support a loan and CashDeck requests complete hundreds of interactions with a bank's portal to retrieve the required data. Without CashDeck, these actions need to be replicated by a client to retrieve this data manually. Manually provided data requires significant extra processing by mortgage brokers and consumers and can increase the time to complete a loan application by multiple days.

Screen scraping is often described as insecure however, in both our research and the research done by ASIC during their last review of the ePayments code, it was noted that there's never been a data breach attributable to mishandling bank credentials by a screen scraping provider — not just in Australia, but worldwide.

Whilst CDR eliminates the risk of leaked credentials, many banks have already mitigated this for screen scraped data by requiring multi-factor authentication on login and for initiating transactions. These codes can only be used once so even in the unlikely event that credentials were compromised, they would be useless.

Once captured, CDR-derived data has the same risk of compromise as screen scraped data. There are no extra protections granted to CDR that make it less susceptible to data loss through compromised datasets, logs, etc than scraped data.

Recommendations to ban scraping appear to be based on the *idea* that sharing credentials is bad, rather than evidence or case studies of that being true. Neither CashDeck nor the government reviews listed in the discussion paper can find evidence to prove that screen scraping has caused any harm or put consumers at higher risk.

Those calling for screen scraping to be banned appear to have vested interests in that outcome, either because they've predicated their business around CDR-only data access without the competition of screen scrapers who currently have access to superior data, or they are data holders who prefer the regulatory and financial hurdles that prevent consumer data (which many institutions see as proprietary to them) being easily accessed by competitors.

Screen scraping is hard. It's much easier to access data via well-defined APIs. CashDeck doesn't use screen scraping because it's easier, quicker, or cheaper than CDR. We do it because its currently the only option to provide the data required for loan applications with the most acceptable user experience.

CashDeck looks forward to a future where our clients can access data directly from institutions via APIs in a standardised and federated manner with the data, capabilities, and user experience currently possible via screen scraping. Until this is possible however, it is important that mortgage brokers be able to continue to access the data they require as part of their compliance and loan application obligations via screen scraping.

WHO IS CASHDECK

As a private company founded in 2014, CashDeck provides solutions for finance brokers and advisers throughout Australia.

We focus on services to assist mortgage brokers meet their obligations under National Consumer Credit Protection Act 2009 s.117 (a-c)[1] and RG 273 (Best Interests Duty)[2] and to gather documentation required by lenders for loan applications.

CashDeck has more than 6,500 users and we estimate our services are used to support between 15-25% of mortgage broker-originated mortgages in Australia.

How We Help Brokers

The services relevant to this discussion paper we provide to brokers include:

1. Enhanced and categorised banking transaction data of applicants used to pre-fill loan applications.
2. Analysis of income and living expenses to ensure NCCP s.117(c) compliance with the accuracy of data provided by the client and RG 273 (BID) for product appropriateness and serviceability requirements.
3. High-level customer-specific product data (including start/end dates of loans, current interest rates and if they're fixed or variable, ending dates for interest only or fixed interest period, ownership information, repayment amounts, current and redraw balance amounts)

[1] National Consumer Credit Protection Act 2009: https://www.legislation.gov.au/Details/C2020C00215

[2] Regulatory Guide 273 (Mortgage brokers: Best interests duty): https://download.asic.gov.au/media/5641325/rg273-published-24-june-2020.pdf

4. Retrieval of official statements and interim statements (as PDFs) from banks used for:

    a. evidence of ownership and balance of savings, offset, transaction, credit card or other accounts not available via Comprehensive Credit Reporting to the lender;

    b. evidence of spending behaviour when required by lender, especially for those customers with high Loan to Value Ratios (LVR) for a lender to ensure adequate loan serviceability.

To facilitate this, CashDeck retrieves data from banks via screen scraping technology. With the current state of CDR, this is still the only way to retrieve the above required data from all account types and ownership structures in Australia with the least amount of friction to customers.

To ensure security, CashDeck only holds user banking credentials temporarily and are securely deleted once the data is retrieved.

We treat consumer data with reverence. All data is encrypted in transit and at rest and staff and users are only granted access to data based on the principle of least privilege[3]. We also hold insurances against a potential breach, but as our continued commercial existence relies extensively on data security and so this is of utmost importance to us.

Contact Details

Wayne Robinson
CTO and Founder
wayne.robinson@cashdeck.com.au
0406 330 316

Level 1, 310 Edward Street
Brisbane QLD 4000

[3] NIST SP 800-12 Rev. 1: https://csrc.nist.gov/glossary/term/least_privilege

RESPONSES

1(a). What is the scope and purpose of the data that is captured? Is the data that is captured only banking data, or does it include data from other sectors?

CashDeck currently only captures banking data however, this definition may not currently include certain lenders. For example, Buy Now Pay Later (BNPL) and other Small Amount Credit Contracts (SACC) or certain credit card types like American Express.

For some services, we also capture data from share trading, managed wealth and superannuation products for which screen scraping is currently the only capture method as they're not supported by CDR.

2(b). What steps do consumers, screen scraping service providers and businesses using screen scraping take in the screen scraping process? What information is provided to consumers through the process?

Consumers are presented with an interface that allows them to:

1. View and confirm the terms and conditions of using the product.
2. Are presented with which mortgage broker is requiring their data.
3. Securely provide their credentials for each bank they need to include.
4. Consent to which accounts to provide to their mortgage broker.

Mortgage brokers using our product are provided with:

1. Enhanced transaction listings for all banks/accounts consented to by the client for the requested period.
2. Analysis of income and living expenses, used to prefill loan applications.

3. PDF-versions of official statements and interim statements, required by lenders for loan applications.

Mortgage brokers use these documents as part of their own serviceability and loan appropriateness calculations as required to comply with NCCP s.117(a-c) and RG 273 (BID). Brokers are required to keep these documents for a period of time required by their Australian Credit License (ACL) obligations, but may be up to 7 years after they are no longer providing services to that customer. This includes the evidence CashDeck currently provides via screen scraping.

Lenders also often require this information as part of loan applications. This includes requests including, but not limited to:

1. Verified summary of assets, liabilities, income, and expenses.

2. First pages of official statements (PDFs) to verify account ownership and balance of those accounts not included as part of Comprehensive Credit Reporting. This includes transaction/savings accounts, offset accounts, term deposits, credit cards, etc.

3. Full statements for a period of 3+ months where a client is a higher risk (for example, where their Loan to Value Ratio (LVR) is greater than 80%) for them to do their own living expense analysis.

1(c). When is the consumer's data accessed as a one-off, and when is longer-term or ongoing access obtained? Where ongoing access is in place, how are consumers made aware of this and can they cancel access at a later point?

Data is only retrieved at the point-in-time the client completes the process. Once done, credentials are securely deleted and can never be reused.

If a broker requires updated data, they must ask the client to complete the process again.

1(d). Do you use screen scraping for purposes other than data collection (for example to undertake actions on behalf of a customer)?

Data is collected, enhanced, and provided to the mortgage broker. We don't make other use of this data.

2. Are there any other risks to consumers from sharing their login details through screen scraping?

Credentials are always kept separate to the underlying requests and only for the time required to complete the retrieval after which, they are securely deleted.

Banks who are concerned about login security have implemented multi-factor authentication as part of the login process. This process uses one-time codes that are provided by the client and each code can only be used once, making their standard credentials useless past the initial retrieval.

If a bank has implemented multi-factor authentication it obviates the risk of sharing passwords.

What CashDeck finds more concerning is a tendency for banks to have insecure password policies and restrictions. For example, at the time of submission a popular consumer bank only allow 4-6 digit PINs for login and one of the largest banks in Australia only allows for a 6 character, case-insensitive password containing no special characters.

There are many more examples across the banking sector where there are artificially small password limits or rules that suggest that passwords may not be being handled with best practice.

The National Institution of Standards and Technology (NIST) recommends[4], among other requirements:

- All user-generated passwords be a minimum of 8 characters
- Have a maximum of allowable limit of 64 characters
- Should allow all characters (including ASCII and Unicode)
- Pasting of passwords should be allowed so that password managers can be used
- Multi-factor authentication should be used

Many banks fail to implement these basic requirements of password security. Even so, with the processes CashDeck uses to handle credentials, there's minimal risk to the client.

[4] NIST Special Publication 800-63B, Section 5.1.1 – Memorized Secrets

3. Do you have any data, case studies, or further information about the risks of consumers sharing their login details through screen scraping?

No however, this is because we were unable to find any situation where credentials provided to any organisation that accesses financial data via screen scraping, in Australia or internationally, was used for anything but their intended purpose.

From our research, credentials used with reputable services that collect data via screen scraping have never resulted in loss to a consumer in more than a decade of them being in common use.

Furthermore, if a bank has implemented multi-factor authentication (see question 2 above), even the risk of compromised credentials is mitigated.

4. Could you provide any examples of actions your organisation takes to prevent or block screen scraping (if you hold the consumer's data, such as a bank), or when your company's use of screen scraping has been blocked (if you provide screen scraping services or you partner with a screen scraper to provide your services), and why?

From time-to-time banks implement measures to block access to screen scraped access.

Whilst CashDeck recognises there are valid reasons for a bank to implement security measures to detect and block automated access to their banking portals, this can be frustrating to both brokers and consumers that use those services.

Providing data manually, often results in significantly more processing time for a broker and often multiple days of delay to a loan application as clients navigate bank's portals to collect what is required by their broker.

Also, when contacted by a customer about screen scraping, banks will often inform them that screen scraping is not allowed and that they can't use such services. This goes against the recommendations made in the last review ASIC made on the ePayments code[5].

[5] ASIC, Report 718: Response to submissions on CP 341 Review of the ePayments Code: Further Consultation, 7 March 2022.

5. Could you provide any examples of how your organisation or entities you partner with manage the risks associated with screen scraping?

Below are some examples on how CashDeck mitigates the risks associated with screen scraping:

1. Modern encryption is used during all transmission (TLS 1.3) and storage (AES-256) of any data, including between internal systems.

2. Further care is taken with the encryption and transmission of credentials and is kept separate from other consumer data.

3. Only point-in-time data is retrieved, and credentials are securely deleted immediately on completion of that retrieval.

4. Credentials are only used by the screen scraping software itself, are never logged and not accessible by staff. This is audited regularly.

5. The screen scraping software only reads data from a user's portal and do not initiate any actions on behalf of the consumer.

6. Are there other proposed reforms or legal frameworks that relate to the use of screen scraping?

We would welcome a similar change to screen scraping as mentioned in the paper relating to screen scrapers identifying themselves to providers if it would allow more consistent access to those provider's data.

Presently, some banks actively implement measures to detect and block screen scraping, preventing consumers from easily accessing their data for purposes such as loan applications or personal wealth management/budgeting.

Also of concern is the regular practice wherein banks make defamatory statements to customers that using services like CashDeck is inherently insecure and they put their finances at risk when doing so. These statements are inflammatory scaremongering, and we would welcome reforms to the ePayments code with the intention of preventing banks from engaging in this hostile practice.

7. Are there any other international developments that should be considered?

No comment.

8(a). Can you provide examples of data that is being accessed through screen scraping that cannot currently be accessed using the CDR or vice versa?

CDR cannot currently provide the following:

1. Official eStatement and interim transaction listing PDFs. These are required to verify ownership of accounts and/or serviceability to lenders as part of the loan application process.

2. Access to certain lender types, specifically Small/Mediuam Account Credit Contract lenders (like Buy Now Pay Later or some personal/short-term loan providers) who's use can significantly effect the appropriateness and serviceability of a mortgage.

3. Access to certain bank-like institutions like American Express and Diners Club.

4. Access to certain business account types.

   There are more than 2.5 million businesses in Australia, most of which are micro and small businesses who's business finances are intrinsically linked to their personal circumstances. This client type makes up a large number of those using mortgage brokers.

   Not all of these account types are covered by CDR and those that are currently have very limited support.

8(b). Are there particular restrictions related to data use and disclosure under the CDR that influence choices to continue using screen scraping, or vice versa?

Mortgage brokers are currently listed under Trusted Advisers in the current legislation which simplifies the provision of data to them under CDR.

However, other finance broker types are specifically excluded from this status. Whilst these other brokers aren't specifically covered under RG 273, many lenders may still require similar evidence

during a loan application. Also, certain asset finance brokers still have obligations under NCCP s.117(a-c) requiring reasonable measures to be taken to verify the financial data provided by the client.

CDR cannot be used for asset finance brokers without the significant extra burden of them becoming Accredited Data Recipients or by using the Sponsored Accreditation model.

Additionally, mortgage brokers are required to keep the evidence gathered for NCCP/RG 273 for long periods of time, often 7 years after the relationship with that customer has ceased (which could be 42 years after the application of a 35 year mortgage). CDR only allows consumers to grant their consent for a maximum of 12 months and can cancel that at any stage, requiring the Accredited Data Recipient to delete all non-anonymised data. CashDeck's understanding of the legislation is that this also extends to the mortgage brokers who have also received that data.

Whilst CDR allows for certain specific Insights to be kept, mortgage brokers require all underlying evidence that formed the basis of their recommendations to be kept as per NCCP/RG 273 and their Australian Credit License (ACL). This is often well past the consent periods allowed by CDR.

8(c). Are there requirements in other regulatory frameworks that affect the viability of CDR as an alternative to screen scraping?

Answered in 8(b).

8(d). Can you provide suggestions on how the CDR framework could be adjusted so that it is a more viable alternative to screen scraping?

The following factors prevent mortgage brokers from being able to use CDR today:

1. Lenders requiring PDFs of official statements and/or interim statements as part of loan applications.

2. Required institutions missing from CDR (Buy Now Pay Later, Small/Medium Amount Credit Contract providers and some credit/charge card providers like American Express) or entire account classes (i.e. certain business accounts). These all effect the serviceability of new lending.

3. Increased consent friction. For example, joint accounts can require each party consent individually outside of the CDR consent scope, which can be very complicated for consumers and will be specific to each bank.

   Similar consent requirements exist for business accounts (when supported) and could effect a large number of mortgage broker-originated loans.

   Users should be able to approve access to any account they can see inside their banking portal which they could download or otherwise provide access to via other means such as screen scraping.

4. Long-term consent (7-42 years) to underlying data is not possible under CDR. Mortgage brokers can't meet their obligations with the Insights or anonymised data allowable from CDR on expired consent.

The above issues would need to be addressed before mortgage brokers could switch from screen scraped data to CDR.

Importantly, even if lenders were banned from requesting official statements as part of the loan application and were forced to use CDR-provided data instead, it would need to be done in a way that reduces friction and consent-overload for the client. Mortgage brokers will be requesting this data first to make a decision on which lender to recommend to a client after its review. It is important that brokers can then forward this evidence to the lender as part of the loan application process, without a client having to complete another out-of-band CDR request direct from the lender.

CashDeck also considers it important that all finance brokers be included in the category of Trusted Adviser, not just mortgage brokers.

9(a). How should the Government determine if the CDR is a viable alternative?

CDR should be able to support all business cases currently possible with screen scraping by doing one or more of the following:

1. increase the capabilities of the CDR specification;

2. increase the products where CDR support is required;

3. modify the CDR legislation to support the use cases currently only supported by screen scraping;

4. introduce legislation to prevent lenders from requiring documents only available via screen scraping or manually by consumers.

9(b). What are your views on a ban on screen scraping where the CDR is a viable alternative?

CashDeck is in full support of a switch to CDR when its capable of supporting all business and legislative requirements of our clients (primarily mortgage brokers).

CashDeck supports an estimated 15-25% of loan applications with our competitors making up a significant portion of the remainder. If screen scraping was banned before CDR was adequately able replace it, the industry enabling brokers to meet their NCCP/RG 273 obligations as well as the brokers themselves would undergo significant disruption and hardship.

9(c). What timeframe would be required for an industry transition away from screen scraping and why?

Most of the changes required for CashDeck to be able to switch to CDR versus screen scraping need to be implemented by legislators, CDR specification designers, Data Holders or lenders' loan application process teams. We're unable to comment on how long it would take for them to implement the changes required for CDR to be a viable alternative for mortgage brokers.

However, once the above was complete, we estimate it would take CashDeck at least 12 months to become accredited, implement and educate our users on the changes required to use CDR versus screen scraping.